

Phishing Email Analysis & Incident Response Report (Training Project)

1) Executive Summary

During a phishing simulation exercise, an employee received an email impersonating the bank's internal security team. The email contained a malicious link leading to a fake login page designed to harvest user credentials. Full email header analysis, authentication checks (SPF/DKIM/DMARC), routing path investigation, and phishing site inspection were conducted.

Key Findings:

From: Security.Team@bank.com

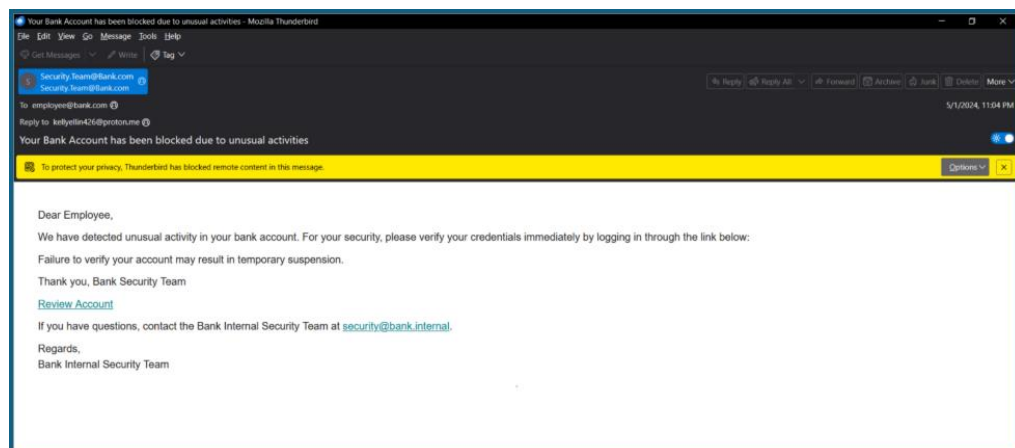
Return-Path / Reply-To: ...@proton.me

SPF = Pass for **protonmail.com** (legitimate sending server)

DKIM = Timeout/Not verified

DMARC = Fail (because neither SPF nor DKIM aligned with the visible From domain bank.com)

Objective: Credential harvesting via a fake portal hosted on a dynamic DNS domain (bankk.ddns.net) with the form posting to save_credentials.php.



2) Email Header Analysis

2.1 Key Fields

From: Security.Team@bank.com (spoofed)

Reply-To / Return-Path: kellyellin426@proton.me → mismatch

Message-ID / X-Mailer: Consistent with ProtonMail

```
From: Security.Team@Bank.com
Date: Wed, 01 May 2024 20:04:05 +0000
Message-ID: <i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMwPAn-HP3FugKsucuswSub00Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>
X-Pm-Message-ID: 55310a2549b19d9ae8e8c9d77c7ff7bf967e0fa21
Subject: Your Bank Account has been blocked due to unusual activities
To: employee@bank.com
Reply-To: kellyellin426@proton.me
Return-Path: kellyellin426@proton.me
```

2.2 Authentication Results

SPF: Pass for protonmail.com

DKIM: Timeout (signature not validated)

DMARC: Fail due to **alignment failure** (From = bank.com, but authentication passed only for protonmail.com).

Operational note: A strict DMARC policy (p=reject) for bank.com would have blocked this.

2.3 Received Path

Multiple hops via Microsoft Exchange and ProtonMail.

Originating IP: 185.70.40.140 (ProtonMail infrastructure, Switzerland, AS62371).

```
Received: from PH7PR14MB5442.namprd14.prod.outlook.com (2603:10b6:510:13e::15) by SA1PR14MB7373.namprd14.prod.outlook.com with HTTPS; Wed, 1 May 2024 20:04:16 +0000
Received: from PA7P264CA0421.FRAP264.PROD.OUTLOOK.COM (2603:10a6:102:37d::22) by PH7PR14MB5442.namprd14.prod.outlook.com (2603:10b6:510:13e::15) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7519.34; Wed, 1 May 2024 20:04:14 +0000
Received: from SA2PEPF00001509.namprd04.prod.outlook.com (2603:10a6:102:37d:cafe::c1) by PA7P264CA0421.outlook.office365.com (2603:10a6:102:37d::22) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7544.25 via Frontend Transport; Wed, 1 May 2024 20:04:13 +0000
Authentication-Results: spf=pass (sender IP is 185.70.40.140) smtp.mailfrom=protonmail.com; dkim=timeout (key query timeout) header.d=protonmail.com;dmARC=pass action=none header.from=protonmail.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of protonmail.com designates 185.70.40.140 as permitted sender) receiver=protection.outlook.com; client-ip=185.70.40.140; helo=mail-40140.protonmail.ch; pr=C
Received: from mail-40140.protonmail.ch (185.70.40.140) by SA2PEPF00001509.mail.protection.outlook.com (10.167.242.41) with Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.7544.18 via Frontend Transport; Wed, 1 May 2024 20:04:11 +0000
X-IncomingTopHeaderMarker: OriginalChecksum:C17AD509B4FA1C33AD6837AF53B05160C3206DAEAS97C784A116FBD1E13D3CAA;UpperCasedChecksum:255DA5C4E53258A65E29BCEB32930DEF55AE003B9737CDFDDA32BCBDDF73A9;SizeAsReceived:1160;Count:10
From: Security.Team@Bank.com
Date: Wed, 01 May 2024 20:04:05 +0000
Message-ID: <i7g9MMh5NtErtaOzQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMwPAn-HP3FugKsucuswSub00Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>
X-Pm-Message-ID: 55310a2549b19d9ae8e8c9d77c7ff7bf967e0fa21
Subject: Your Bank Account has been blocked due to unusual activities
To: employee@bank.com
Reply-To: kellyellin426@proton.me
Return-Path: kellyellin426@proton.me
```

2.4 WHOIS & GeolIP

Reverse DNS: 185-70-40-140.protonmail.ch

Organization: Proton Technologies AG (Switzerland)

Abuse contact: abuse@protonmail.ch

Responsible organisation: [Proton AG](#)

Abuse contact info: abuse@protonmail.ch

```
inetnum:      185.70.40.0 - 185.70.40.255
netname:      protonmail-1
descr:        Proton Technologies AG
country:      ch
admin-c:      PLA68-RIPE
tech-c:       NA7583-RIPE
status:       ASSIGNED PA
mnt-by:       protonmail-mnt
mnt-routes:   protonmail-mnt
created:      2014-09-16T08:07:21Z
last-modified: 2024-07-31T12:58:35Z
source:       RIPE
```

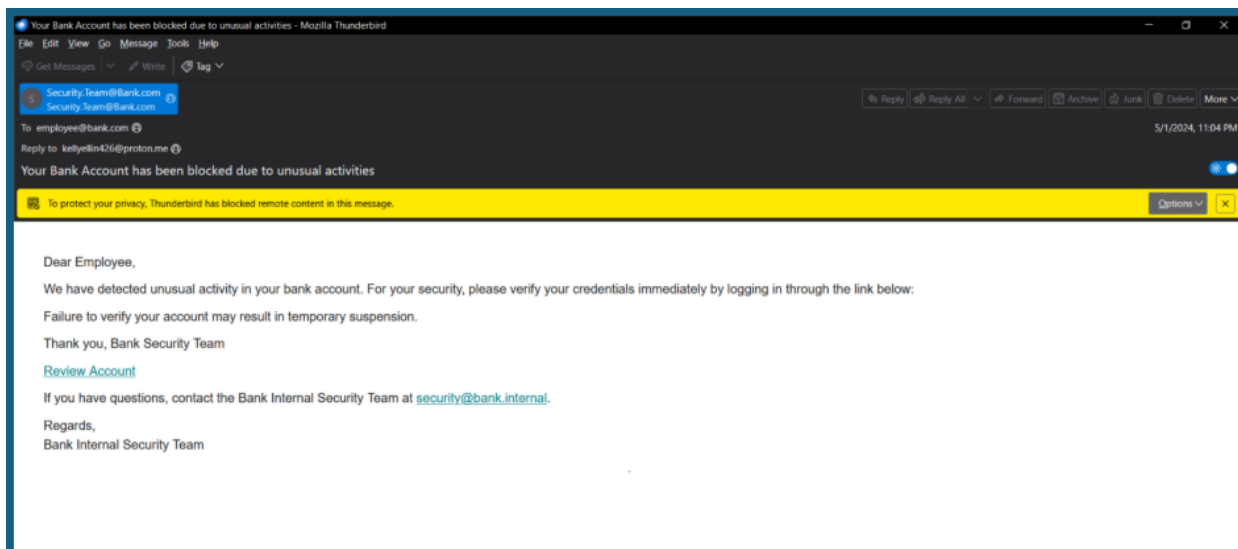
3) Email & Landing Page Content Analysis

Subject: "Your Bank Account has been blocked due to unusual activities"

Style: Urgent tone, scare tactics

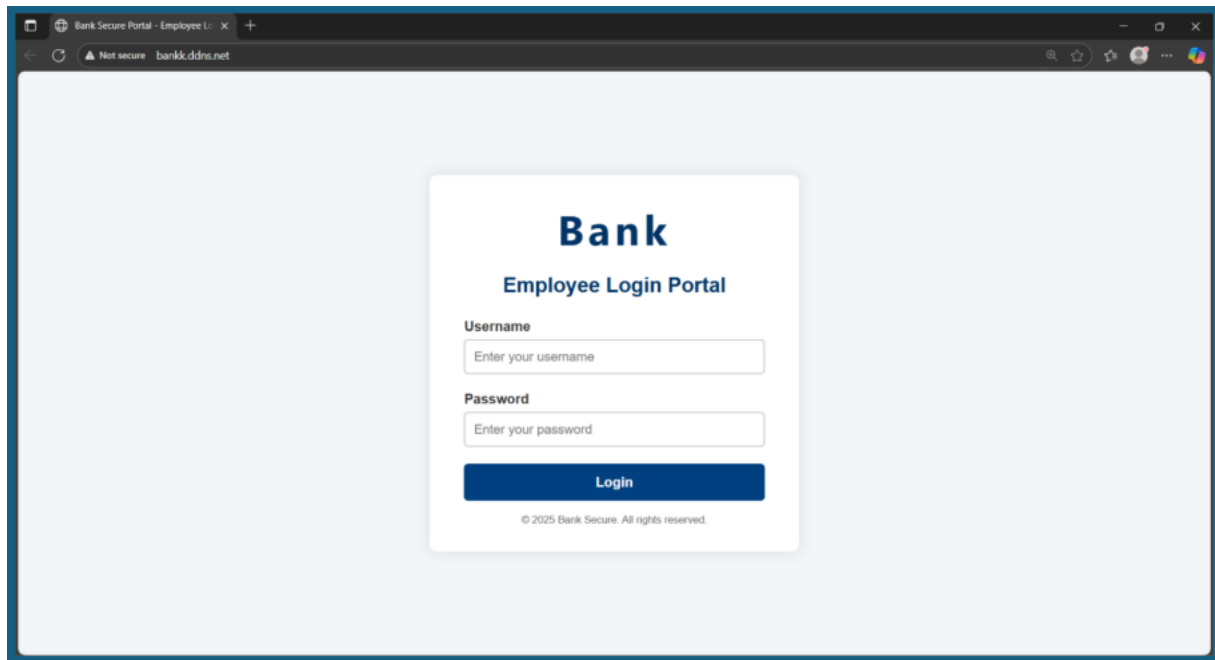
Link: <http://bankk.ddns.net/> (dynamic DNS domain, not official bank)

Fake contact: security@bank.internal (non-existent internal domain)



3.1 Fake Login Page UI

Mimics the bank's portal design.
Lacks HTTPS trust indicators.



3.2 Page Source Code

Form action: save_credentials.php
Collects entered credentials.

```
    }  
    </style>  
</head>  
<body>  
    <div class="login-container">  
        <div class="logo-text">Bank</div>  
        <h2>Employee Login Portal</h2>  
        <form method="POST" action="save_credentials.php">  
            <label for="username">Username</label>  
            <input type="text" id="username" name="username" placeholder="Enter your username" required />  
  
            <label for="password">Password</label>  
            <input type="password" id="password" name="password" placeholder="Enter your password" required />  
  
            <input type="submit" value="Login" />  
        </form>  
        <div class="footer">© 2025 Bank Secure. All rights reserved.</div>  
    </div>  
</body>  
</html>
```

4) Technical Deep-Dive

4.1 Link Analysis


Dynamic DNS (bankk.ddns.net) used for hosting.
Easier for attacker to swap IPs and evade static IP blocks.

4.2 Domain/IP Analysis

Domain: bankk.ddns.net
Mail Source IP: 185.70.40.140 (ProtonMail)
ASN: 62371
PTR: 185-70-40-140.protonmail.ch

IP Information for 185.70.40.140

— Quick Stats

IP Location	 Switzerland Plan-les-ouates Proton Technologies Ag
ASN	 AS62371 PROTON Proton AG, CH (registered Nov 17, 2015)
Resolve Host	185-70-40-140.protonmail.ch
Whois Server	whois.ripe.net
IP Address	185.70.40.140

5) Indicators of Compromise (IOCs)

Type	Value	Notes
Domain	bankk.ddns.net	Malicious DDNS domain
URL	http://bankk.ddns.net/	Phishing landing page
IP	185.70.40.140	ProtonMail shared infra
Reverse PTR	185-70-40-140.protonmail.ch	ProtonMail hostname
ASN	62371	Proton Technologies AG
Abuse Contact	abuse@protonmail.ch	For abuse reporting

6) Timeline & Metrics (Simulation)

Time (AST)	Event
09:12	User report received, IR ticket opened
09:15	Triage, email quarantined
09:28	Header analysis → DMARC fail confirmed
09:35	Sandbox inspection of phishing link
09:44	IOC extraction complete
09:52	Transport Rules updated (From≠Return-Path + DMARC fail)
10:03	Blocked bankk.ddns.net on URL Filter
10:10	User awareness notification

MTTA: ~3 min | **MTTR:** ~58 min (simulated)

Note: Some steps (e.g., Transport Rules, URL Filtering) were not executed but documented to reflect realistic procedures. All times are simulated.

7) Incident Response Steps

Containment

- Quarantined the phishing email.
- Transport Rules: block if From≠Return-Path + DMARC fail.

Verification

- Verified SPF/DKIM/DMARC misalignment.
- Abuse contact notification sent (ProtonMail)

Eradication & Recovery

```
PS C:\WINDOWS\system32> New-NetFirewallRule -DisplayName "Block Malicious IP" -Direction Inbound -Action Block -RemoteAddress 185.70.40.140
>>

Name                : {c52772e7-ad2e-42d0-b243-f86db4a0f7e3}
DisplayName          : Block Malicious IP
Description          :
DisplayGroup         :
Group                :
Enabled              : True
Profile              : Any
Platform             : {}
Direction            : Inbound
Action               : Block
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses :
PolicyAppId          :

PS C:\WINDOWS\system32> Get-NetFirewallRule -DisplayName "Block Malicious IP" | Get-NetFirewallAddressFilter
>>

LocalAddress : Any
RemoteAddress : 185.70.40.140
```

Blocked domain on Secure Web Gateway.

Blocked malicious IP manually.

Reported abuse to abuse@protonmail.ch.

Reviewed logs, enforced password reset if required.

Verified SPF/DKIM/DMARC misalignment.

Note: In this case, the malicious IP and domain were blocked manually as part of containment. However, such phishing attempts could also be detected and mitigated automatically using SIEM detection rules (e.g., Sigma for From/Return-Path mismatch with DMARC failure) or KQL queries in Microsoft 365 Defender.

8) Recommendations

Enforce **DMARC p=reject** with aligned SPF/DKIM.

Enable **external tagging** ([EXTERNAL]) on inbound emails.

Transport Rules to reject spoofed @bank.com messages.

Quarterly **phishing awareness training**.

Secure Web Gateway to block DDNS/Phishing categories.

9) Risk & Impact

Potential Impact: Credential theft → unauthorized account access.

Mitigation: MFA, Conditional Access, anomaly detection.

If compromise suspected: Reset credentials, invalidate sessions, review logs.

10) Legal & Ethical Considerations

This was a **controlled training exercise**.

Abuse reporting performed only via official contacts.

11) Redacted Header Excerpt

From: Security.Team@bank.com

Reply-To: kellyellin426@proton.me

Return-Path: [<kellyellin426@proton.me>](mailto:kellyellin426@proton.me)

Authentication-Results: spf=pass smtp.mailfrom=protonmail.com; dkim=timeout; dmarc=fail (alignment)

Received: from mail-185-70-40-140.protonmail.ch (185.70.40.140)

12) MITRE ATT&CK Mapping

T1566.002 – Spearphishing Link (primary technique)

T1056.002 – Input Capture: Web Forms (credential harvesting)